Certificación electrónica aplicada en Venezuela y su legislación: garantías y desventajas para negociaciones seguras

Silva Dugarte, María Fernanda[1]

Recibido: 11/06/2010 • **Revisado:** 15/07/2010
Aceptado: 18/10/2010

Resumen

El presente artículo tiene como objetivo fundamental evaluar el sistema de certificación electrónica aplicado en Venezuela y su legislación, así como dar a conocer las garantías y desventajas que provee el sistema de certificación electrónica a los usuarios, específicamente, cuando se ejecutan actividades que van a producir efectos jurídicos. El diseño de la presente minuta investigativa obedece a un corte documental a nivel descriptivo, por cuanto los datos fueron extraídos de textos legales especializados en la materia. A través de la presente investigación se puede concluir que el sistema de certificación electrónica se ha convertido en un aliado para los usuarios en el ciberespacio y su empleo es obligatorio para brindar mayor seguridad y certeza jurídica a las operaciones realizadas vía internet.

Palabras clave: certificación electrónica, ciberespacio, proveedores de certificación electrónica, firma electrónica, certificado electrónico.

Abstract

ELECTRONIC CERTIFICATION APPLIED IN VENEZUELA AND ITS LEGISLATION: GUARANTEES AND DISADVANTAGES FOR NEGOTIATIONS SAFE

The main purpose of this investigation is to study the foundations of the electronic certification system used in Venezuela, its corresponding legislation and likewise the guarantees and disadvantages that users have and particularly, when they perform operations that involve legal matters. The design of the present investigative paper complies with a documentary cut at a descriptive level since the information was extracted from legal texts specialized in the matter. Based on the findings of this research we can conclude that the electronic certification system has become an ally to cyberspace users, its use is mandatory when providing more security and legal certainty to transactions carried out via Internet.

Keywords: *electronic certification, cyberspace, providers of electronic certification, electronic signatures, electronic certificates.*

1 Especialista en Derecho Mercantil de la Universidad de Los Andes (2011), Abogada, Profesora invitada de la Cátedra de Legislación Organizacional de la Escuela de Administración y Contaduría Pública, Faces-ULA. E-mail: mfernandas@hotmail.com

1. Introducción

Los crecientes y vertiginosos avances tecnológicos y comunicacionales que se han venido evidenciando con el uso del internet durante las últimas décadas, han conllevado la adaptación de la vida en sociedad al nuevo mundo de la red. Este medio ha permitido ahorrar tiempo, dinero, espacio y/o distancia en la realización de operaciones comerciales, administrativas y de toda índole, al tiempo que se exige y se espera seguridad jurídica y práctica para que dichas operaciones puedan ser equivalentes a las comúnmente realizadas por las vías tradicionales. La trascendencia de las innovaciones en matera electrónica con respecto a la transferencia de datos en tiempo real, ha transitado de ser una actividad de simple interés tecnológico, hasta transformarse en objeto de análisis desde los puntos de vista académico, económico, político, social y hasta jurídico.

Estas razones dieron lugar en Venezuela, a la promulgación del Decreto –Ley de Mensajes de Datos y Firmas Electrónicas (LMDFE, 2001) y su respectivo Reglamento, en aras de propagar el uso adecuado de las Tecnologías de la Información y Comunicación (TIC) que sin lugar a dudas han incluido todas las áreas del conocimiento humano y han eliminado las fronteras físicas. Dicha legislación tiene como objetivo primordial brindar un marco jurídico mínimo e indispensable para las actividades relativas a la transmisión de información a través de medios electrónicos, para que de esta manera, todos los sujetos intervinientes en el proceso puedan contar con un instrumento legal que le adjudique validez jurídica a sus operaciones. Dicha legislación contempla la creación de un sistema de certificación electrónica cuyo objetivo es ofrecer seguridad y valor probatorio a las operaciones que se realicen vía internet, con la firme convicción de que los usuarios hagan uso del mismo para que sus actividades en el ciberespacio sean reconocidas judicialmente en caso de controversias. Esta realidad atañe a las sociedades mercantiles al momento de realizar negociaciones, puesto que con el avance de la tecnología éstas han tenido que recurrir a la utilización de la web, el internet, para ofrecer sus servicios y productos a los consumidores. De allí, pues, la necesidad de contar con una herramienta en Venezuela que ofrezca garantía en la utilización de intercambio de información para cerrar negociaciones transcendentales.

2. Funcionamiento del Sistema de Certificación Electrónica aplicado en Venezuela de acuerdo a la legislación patria

El 26 de mayo del año 2010, fue publicada en la Gaceta Oficial Nº 39.432, la providencia Nº 004-10 emanada de Superintendencia de Certificación Electrónica (SUSCERTE, 2010 [a]: 3), que contempla en su artículo 2, lo siguiente:

> A los fines de garantizar el cumplimiento de lo establecido en los artículos 1, 4, 5, 7 y 8, de la ley sobre mensajes de datos y firmas electrónicas se hace imperante que toda firma electrónica, mensaje de datos e información inteligible en formato electrónico emitidos en Portales y Sistemas de Información de Instituciones Públicas o Privadas, que ameriten eficacia, valor jurídico, protección de la integridad de la información y garantizar su autoría, deberán estar en la cadena de confianza de certificación electrónica, avalada por un Proveedor de Servicios de Certificación debidamente acreditado ante esta Superintendencia.

En virtud de lo expuesto, los mensajes de datos[2], correos electrónicos[3] y demás transacciones de semejante naturaleza, para los cuales se requiera que cumplan o generen consecuencias jurídicas para las instituciones y usuarios, sean éstos públicos o privados, deberán obligatoriamente someterse a lo establecido por dicha providencia. Esta exige el uso de firmas electrónicas en el caso de usuarios y representantes de empresas públicas o privadas, así como también, la certificación electrónica de procesos o transacciones en el caso de empresas o entidades públicas y/o privadas.

De esta manera, se demuestra claramente la obligatoriedad de la existencia de los sistemas de certificación electrónica. Sin embargo, es menester señalar que existen condiciones en las cuales los mismos pueden o no intervenir en las operaciones realizadas en la web, y a tal fin se debe hacer referencia al ámbito de los sistemas de encriptación[4], los cuales se pueden clasificar de la siguiente forma:

2.1 Sistema de encriptación simétrica

También denominado **sistema de clave compartida**, es aquel en el cual tanto el emisor como el remitente o destinatario de un mensaje de datos, hacen uso de la misma clave para encriptar y desencriptar el mensaje, por consiguiente, constituye el procedimiento más sencillo de cifrado por cuanto la misma clave sirve tanto para cifrar como para descifrar la información. Es ideal para brindar un estándar de seguridad suficiente en el caso de que las partes involucradas se conozcan previamente, y por lo tanto, basen sus relaciones en el principio de la confianza mutua. Por ello, "implica una relación cerrada a determinados intervinientes que han acordado esta forma de contratar entre ellos y que se han comunicado las correspondientes claves" (Recalde, 2006: 76). No obstante, en el campo de las redes abiertas de internet "no es recomendable el uso de este sistema, sino al contrario, es preferible que la clave sólo se encuentre a disposición de su correspondiente titular sin que la otra parte conozca su contenido" (Chacón, 2005: 61).

2.2 Sistema de encriptación asimétrica

También denominado **sistema de clave pública**, en el cual prevalecen dos tipos de claves: una pública que no es secreta, es de libre acceso y cuya función se cierne en encriptar el mensaje, y una privada que sólo conoce el usuario al cual pertenece, por consiguiente, debe permanecer en secreto y su objetivo es desencriptar el mensaje. Se trata de un método que garantiza que ese par de claves sólo se pueden generar una vez, de modo que se puede inferir que es imposible que dos personas obtengan por casualidad la misma pareja de claves. Por tal motivo, "con este sistema se evitan los riesgos de comunicar claves secretas o de su pérdida, con lo que se abre enormemente el ámbito de los posibles intervinientes en la operación" (Recalde, 2006: 77).

Este es precisamente el sistema aplicado en Venezuela para todas las transacciones electrónicas de acuerdo a lo establecido en la legislación patria, con la creación de los proveedores de servicios de certificación[5]

2 Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.
3 Servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónica.
4 Es un proceso, generalmente digital, en el que realizándose un cálculo matemático, sobre la base de un algoritmo, se lleva a cabo el cifrado de un mensaje electrónico de forma que sólo es posible el descifrado, esto es, el acceso al mensaje original, mediante la aplicación del correspondiente algoritmo o clave para realizar el proceso inverso.
5 Persona dedicada a proporcionar certificados electrónicos y demás actividades previstas en el Decreto de LMDFE.

regulados a partir del Capítulo VI del Decreto-LMDFE (2001). Se trata de un sistema que se ha extendido por el mayor nivel de seguridad que ofrece a las operaciones realizadas en redes abiertas, garantizando que sólo se abre un documento electrónico si se recibe íntegro e inalterado, por lo que Madrid (2001: 1198) sostiene que:

> …el procedimiento garantiza que cuando se accede a un documento electrónico mediante la utilización de la clave pública el mismo ha sido recibido en su integridad e inalterado. El tercero que utiliza la clave pública tiene la seguridad de que el documento corresponde al titular de la clave privada.

Por otra parte, de acuerdo a Pinochet (2001: 38):

> Al aplicar la firma digital sobre un documento, ésta se mezcla o confunde con los datos que son enviados a través de un proceso de encriptación de la información. Al llegar el mensaje a su destino el mensaje se desencripta con la clave pública que se asocia a la clave privada de su autor. La clave pública podrá ser accesible por cualquier persona incluso en bancos de datos que serán consultados vía Internet.

Ahora bien, todo lo anteriormente explicado puede perfectamente resumirse de la siguiente manera: se tiene en principio un mensaje claro, al que el emisor y firmante del mismo le aplica la clave pública del destinatario -que reposa en un directorio de carácter abierto dispuesto por los proveedores de servicios de certificación electrónica- lo cual conduce a la formación del cifrado del mensaje. Una vez que la información llega al destinatario, éste le aplicará su clave privada al mensaje para desencriptarlo y poder tener para sí el mensaje claro. Del mismo modo, gracias a la intervención del proveedor de servicios de certificación electrónica, el destinatario podrá recibir el mensaje sin alteraciones y con plena conciencia de que efectivamente el autor de la firma es quien alega serlo, por cuanto a través de la emisión de un certificado electrónico[6], el proveedor de servicios da fe de quién es el signatario del mensaje, lo cual posteriormente garantiza el no repudio de la información contenida en el mismo y su autenticidad. Así, tal como lo establece el último aparte del artículo 34 del Decreto-LMDFE: "Los Certificados Electrónicos proporcionados por los Proveedores de Servicios de Certificación garantizarán la validez de las Firmas electrónicas[7] que certifiquen, y la titularidad que sobre ellas tengan sus signatarios" (p.30).

Se debe tener en cuenta que a pesar de que numerosos autores han sostenido una sinonimia entre el sistema de encriptación y la firma electrónica, tal afirmación es errónea, por cuanto la firma electrónica sólo tiene como función declarar la autoría del mensaje de datos. En otras palabras, señalar quién es al autor o emisor del mismo, en caso de que éste sea el mismo signatario; y el sistema de encriptación es un método que permite, a través de la utilización en este caso particular de dos claves (una pública y una privada), asegurar el contenido del mensaje de datos permitiendo que éste llegue íntegro y sin alteraciones a su destino, conservando la información explanada en el mismo. La inverosimilitud de la primera afirmación es fácil de demostrar con sólo contemplar la idea de que efectivamente

6 Mensaje de datos proporcionado por un Proveedor de Servicios de certificación electrónica que le atribuye certeza y validez a la Firma Electrónica.

7 Información creada o utilizada por el Signatario, asociada al Mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

"existen mensajes de datos firmados y cifrados al mismo tiempo, así como también, mensajes de datos cifrados sin ser firmados, como por ejemplo, los correos electrónicos" (Centeno, 2009: 17).

En el mismo orden de ideas es importante acotar que el uso de estas claves asimétricas solamente permite establecer el vínculo de una clave con otra, pero de ninguna manera garantiza que el sujeto que dice ser el propietario de un par de claves, sea efectivamente el dueño, lo cual da lugar a la posibilidad de que se suscite la suplantación de identidades. A tal fin, para dar con la identificación real de una clave pública con un determinado sujeto, se hace necesaria la intervención de los Proveedores de Servicios de Certificación Electrónica, cuyo objetivo se cierne en emitir certificados electrónicos, es decir, implementar "la certificación electrónica que vincula unos certificados de verificación de firma a un signatario o firmante y confirme su identidad" (Rodríguez, 2001: 66), brindando de esta forma un nivel de seguridad y confianza similar al alcanzado en las transacciones realizadas de forma tradicional.

Visto de esta forma, se pueden claramente distinguir, en resumen, los sujetos intervinientes en la estructura del sistema asimétrico consagrado en la legislación nacional, a saber: signatario[8], destinatario[9] y certificador. En primer lugar está el signatario, que no es más que el autor de la firma electrónica, siendo el titular o tenedor exclusivo de una clave privada; en segundo lugar, el destinatario que viene a ser el sujeto a quien va dirigido el mensaje de datos, tal como lo establece el Decreto-LMDFE en su artículo 2; y por último, el certificador, que es un elemento típico integrante de los sistemas con infraestructura de clave pública, y al que se le ha denominado Proveedor de Servicios de Certificación Electrónica en ocasión del argot jurídico venezolano, cuya función radica en legitimar la autenticidad del mensaje y de la identificación cierta del signatario.

Por otra parte, destacan algunas premisas de carácter jurisprudencial relativas a la certificación electrónica en Venezuela, a saber**:**

- Decisión 2188-27-AP21-L-2008-002697 de fecha 27 de abril de 2009 del Tribunal Trigésimo de Sustanciación y Ejecución del Circuito Judicial del Trabajo del Área Metropolitana de Caracas[10], en cuanto a solicitud de parte interesada para la notificación del demandado a través de medios electrónicos, donde se reafirma la función de los proveedores de servicios de certificación electrónica y se rechaza la solicitud por cuanto el tribunal se pregunta ¿quién es el emisor? y ¿dónde está la cuenta de correo electrónico emitida por un proveedor de servicios de certificación que sea de carácter público?. Tendría el Tribunal que crear una cuenta de correo electrónico, y no existiendo un proveedor de servicios de certificación electrónica para los organismos jurisdiccionales del Estado tal como lo estipula el artículo 3 del Decreto-LMDFE.

En este caso, no existirían las debidas garantías procesales para las partes, por cuanto una de ellas actualmente se encuentra en "desventaja procesal", en el sentido de

8 Es la persona titular de una Firma Electrónica o Certificado Electrónico.
9 Persona a quien va dirigido el Mensaje de Datos.
10 Disponible en: http://www.tsj.gov.ve/decisiones/2009-2010

que no se podría determinar con exactitud la fecha exacta en la cual la parte – en este caso particular, el demandado- quedó notificada, para entonces efectivamente comenzar con el cómputo de los lapsos para fijar la celebración de la audiencia preliminar. A tenor de lo expresado anteriormente se transgrede el derecho a la defensa establecido en la Carta Magna y así mismo se violenta el principio procesal de igualdad entre las partes.

-Decisión 2268-6-AP-R-2010-000108 de fecha 6 de abril de 2010 del Tribunal Superior Octavo del Circuito Judicial del Área Metropolitana de Caracas[11], en cuanto a la experticia informática, declarando a lugar la aceptación de unos correos electrónicos almacenados en un dispositivo de almacenamiento masivo USB (Pendrive) como prueba. En tal caso, se oficia a la SUSCERTE para que a través de funcionario capacitado en la materia, haga la respectiva experticia que conlleve a la comprobación de los datos que conforman dichos correos electrónicos y emita la certificación a que haya lugar. En todo caso, ha sido necesaria la intervención de éstos entes por parte de quienes dirimen conflictos ante los órganos jurisdiccionales del Estado, que actualmente carecen de los recursos, o medios para poder, directamente, declarar la veracidad de la información que se presenta como elemento probatorio.

-Providencia Administrativa Nº 052 emanada de la Comisión Nacional de Casinos, Salas de Bingo y Máquinas Traganíqueles (2010), publicada en la Gaceta Oficial Nº 39.499 de fecha 18 de junio de 2010, establece que las licenciatarias están en la imperativa obligación de utilizar los certificados electrónicos y firmas electrónicas con el objeto de garantizar el adecuado uso de las tecnologías de la información y la comunicación en el intercambio de información y trámites administrativos de diversa índole entre las empresas de casinos, salas de bingo y máquinas traganíqueles. Esto, en aras de mantener estándares adecuados de confidencialidad, autenticidad, integridad y control de la información.

Con todo, se demuestra ampliamente lo puntual que resulta ser la intervención de los proveedores de servicios de certificación electrónica en el proceso de encriptación asimétrica y de su imperativa existencia en la legislación patria. En este sentido, a través de la emisión de certificados electrónicos, se garantiza la identidad del sujeto firmante del mensaje de datos signado, así como también la confidencialidad y la integridad de la información transmitida por medio de la red.

Por último, es importante reiterar una vez más que bajo ninguna circunstancia la naturaleza de los certificados electrónicos emitidos por los proveedores de servicios de certificación, puede considerarse similar a la de los documentos públicos (autenticados o protocolizados) puesto que son expedidos por una persona que carece de facultades de fedatario público, es decir, no es notario ni registrador. Sin embargo, acredita la validez del intercambio y manejo de información a través de las redes electrónicas, siendo esta afirmación fundamentada en que la legislación especial venezolana en materia electrónica le adjudica a los mensajes de datos, normas constitucionales y legales que avalan el derecho de acceso a la información personal y a la privacidad de las comunicaciones. Así pues, otorga eficacia probatoria, presentándose ésta de la siguiente manera: a) el mensaje de datos en sí mismo será evaluado bajo el

11 Disponible: http://www.tsj.gov.ve/decisiones/2009-2010

criterio de las pruebas libres, en el sentido de que el jurisdicente calificará la misma y otorgará así valor probatoria a la misma cuando lo considere pertinente y se permite su promoción en los procesos judiciales; b) el contenido de un mensaje de datos plasmado en papel, se considera con la misma eficacia probatoria que tienen las reproducciones fotostáticas y las copias; c) la obligatoriedad de que para la existencia del mensaje de datos se haya hecho uso de la encriptación y que el mismo sea respaldado por un certificado electrónico, mecanismos que son provistos por un Proveedor de Servicios de Certificación; y para que el mensaje de datos pueda ser utilizado como medio de prueba, tiene que cumplir cabalmente con las condiciones de inteligibilidad, conservación, disponibilidad y buen funcionamiento tanto del computador de donde emana como del computador a donde tiene fijado su destino, además del requisito de autoría, es decir, existencia de una firma electrónica.

3. Instituciones venezolanas acreditadas para proveer servicios de Certificación Electrónica

La SUSCERTE (2010[a]), desarrolla un plan estratégico de investigación, información y desarrollo destinado a la producción eficiente de seguridad en materia electrónica y entre sus parámetros establece que:

> …se estructura a partir de un conjunto de líneas y proyectos de investigación que tienen como propósito fundamental, impulsar en su máxima expresión el desarrollo de dos grandes áreas estratégicas del conocimiento, a saber: la Certificación Electrónica y la Seguridad de la Información. Para ello se pretende, promover y formar grupos interdisciplinarios e interinstitucionales de investigación y formación, que amparados en modelos, procedimientos y métodos científicos, otorguen niveles de seguridad y validez jurídica a los Mensajes de Datos y a las Firmas Electrónicas, conforme a lo establecido en el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas [Documento en línea].

Es decir, que la Superintendencia creada en Venezuela con el propósito de coadyuvar con el otorgamiento de legalidad de las transacciones y cualquier intercambio de información a través de la web, acreditará instituciones -sean estas de carácter público o privado- previo cumplimiento de ciertos requisitos establecidos en el Decreto-LMDFE.

La SUSCERTE (2010[b]), como ente rector en materia de servicios de certificación electrónica, en el año 2007 dio origen a la creación de la *Autoridad Certificadora Raíz del Estado Venezolano*, con la finalidad de facultarla para la acreditación de proveedores de servicios de certificación. El objetivo para lo cual fue creada, se resume en verificar el cumplimiento de requisitos y parámetros exigidos por SUSCERTE para poder acreditar a proveedores de servicios de certificación en Venezuela y para que éstos a su vez validarán el intercambio de información a través de la web, de igual manera, entre sus facultades se encuentran:

Emitir, renovar, revocar y suspender los certificados electrónicos a:

> La propia Autoridad de Certificación Raíz del Estado Venezolano.
>
> Las Autoridades de Certificación de los Proveedores de Servicios de Certificación

Acreditados, una vez que éstos cumplan los requisitos establecidos en el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas y su Reglamente Parcial y obtenga su Acreditación. Las Autoridades de Certificación para casos especiales en proyectos de interés nacional.

Las Autoridades de Certificación principales de los Proveedores de Servicios de Certificación Acreditados están subordinadas a la Autoridad de Certificación Raíz del Estado Venezolano, siendo por ende, el segundo nivel de la Infraestructura Nacional de Certificación Electrónica.

Las Autoridades de Certificación podrán emitir, renovar, revocar y suspender los certificados electrónicos a los signatarios y a sus Autoridades de Certificación subordinadas, de acuerdo a lo establecido en la Declaración de Prácticas de Certificación y Políticas de Certificados aprobadas por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), al Proveedor de Servicios de Certificación Acreditado [Documento en Línea]

Es menester hacer referencia a que los certificados emitidos por la autoridad de Certificación Raíz del estado Venezolano, son de carácter público, en el sentido de que estarán disponibles a través de sus portales web, durante un tiempo aproximado de 365 días, durante las 24 horas del día para que puedan ser consultados.

Ahora bien, es preciso acotar que fueron acreditados en el año 2008 dos proveedores de servicios de certificación electrónica, a saber:

3.1 Fundación Instituto de Ingeniería (FII)

Es un ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias, creado en 1980 a través del Decreto Nº 733 de la Presidencia de la República de Venezuela. Se encuentra domiciliada en Caracas, Distrito Capital específicamente "Carretera Nacional Hoyo de la Puerta- Baruta, Urb. Monte Elena II, Altos de Sarteneja" (Urdaneta, 2010, p.29). Fue fundada por la República de Venezuela y organismos como CONICIT, PDVSA, CADAFE (CORPOELEC, actualmente), CANTV, VENALUM, Instituto Venezolano de Investigaciones Científicas (IVIC) y Universidad Simón Bolívar. Su finalidad es la realización de actividades de investigación, desarrollo tecnológico, asesoría y servicios especializados para la industria y el sector público del país, concentrando sus objetivos en las áreas de investigación aplicada al enfoque de la ingeniería y su relación con los requerimientos del desarrollo del país; la formación de personal capacitado y especializado en el área, para crear capital humano técnico y transferencia de tecnología. Todo con la finalidad de fomentar el uso adecuado de la procesos tecnológicos en aras de alcanzar el desarrollo tecnológico y científico de la nación, más específicamente "…ofrece sus servicios principalmente a empresas públicas, organismos gubernamentales, personas naturales y jurídicas" (Urdaneta, 2010: 29).

Es precisamente por su naturaleza y objetivos, que esta institución se conforma en un proveedor de servicios de certificación electrónica de carácter público, acreditado el 11 de julio de 2008 a través de la Providencia Administrativa Nº 027, publicada en la Gaceta Oficial Nº 38.894 del 31 de julio del mismo año, teniendo la obligación de cumplir cabalmente con las exigencias técnicas y requisitos formales establecidos en la legislación aplicable a la materia.

Por tratarse de un proveedor de servicios de certificación electrónica de carácter

público, está exento del pago de las tasas por concepto de su acreditación, renovación o cancelación de ésta y por la autorización que sea otorgada a estos proveedores con respecto a la garantía de los certificados electrónicos proporcionados por proveedores extranjeros, de acuerdo a lo establecido en el artículo 24 del Decreto-LMDFE (2001).

En cuanto a las instituciones venezolanas que han adoptado el uso del sistema de certificación electrónica para así garantizar el eficaz servicio o producto que ofrezca, están:

> "La Oficina Nacional de Identificación y Extranjería (epasaporte), actualmente SAIME, siendo su inicio de ejecución en Venezuela en el mes de Marzo del año 2007, convirtiéndose Venezuela en el primer país del Continente Americano en el empleo de tecnología de pasaporte electrónico y cédula electrónico como documento migratorio ya con el certificado electrónico… *(omissis)*…
>
> "Así mismo, la Contraloría General de la República con la utilización del Certificado Electrónico de la Declaración Jurada de Patrimonio. La Certificación Electrónica en el Servicio Nacional de Contratista el cual se realizará en línea y estará a disposición del público en general a través de la página Web del Servicio Nacional de Contratista". El Caso Villas del Cine a través del Sistema de firma de videos para garantizar los derechos de autor en los formatos digitales, contando actualmente con más de 60 productoras registradas. Y finalmente el caso del Ministerio del Poder Popular para la Alimentación, mediante la aprobación de exportaciones de alimentos de manera electrónica y la solicitud de aprobación de divisas para la exportación de alimentos (CADIVI)". [Disponible en: http://www.suscerte.gob.ve)

Por otra parte es necesario acotar que el Estado Venezolano a través de sus políticas gubernamentales aspira al fortalecimiento de la utilización de la certificación electrónica en sus instituciones, "por lo que actualmente realiza gestiones para implementar el sistema en: PDVSA (Petróleos de Venezuela), Metro de Caracas, Instituto Venezolano de los Seguros Sociales, CADIVI (Comisión de administración de divisas), Ministerio del Poder Popular para las Relaciones Exteriores, Consejo Nacional Electoral". [Disponible en: http://www.suscerte.gob.ve).

3.1.1 Del procedimiento para obtener certificados por parte de Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico (PSC-FII)

Para la obtención de certificados electrónicos (contratación) por parte de FII, es necesario, o bien realizar una cita telefónica para solicitar una reunión en la sede de la institución, o recurrir a la utilización de la página web://ar.fii.gob.ve. En la propia sede de la institución puede realizarse la contratación, consignación de documentos y de depósito bancario y registro de datos. Una vez que el usuario contrata y entrega toda la documentación requerida por parte de la institución, se le provee de una tarjeta criptográfica (con su lectora), software de instalación, copia del contrato general de servicios y su certificado electrónico.

Urdaneta (2010:30), hace especial mención de que el Instituto FII:

> … ha emitido 152 certificados electrónicos al Servicio Autónomo de Registros y Notarías (SAREN), los cuales han sido distribuidos por todo el país y está estipulado que emitan 200 más para cubrir todos los registros y notarías. También se han emitido certificados

electrónicos al Centro Nacional de Tecnología de la Información CNTI, adscrito al MPPCTII, a la Fundación Villa del Cine, a la SUSCERTE, a Venalum en Puerto Ordaz y a la Fundación Instituto de Ingeniería para firmar documentos dentro del Sistema Administrativo Integrado, SAI.

Este instituto por tener el carácter de ente público, autoridad de registro de segundo nivel –SUSCERTE, considerada registro de nivel superior- se caracteriza por proveer de certificados electrónicos a instancias gubernamentales como las mencionadas anteriormente, así como al SENIAT, CADIVI, Metro de Caracas. Sin embargo, es de hacer notar que a pesar de ser un proveedor de carácter público no ostenta la disposición para proveer certificados electrónicos a los organismos jurisdiccionales del Estado, de acuerdo a una opinión general expresada en la decisión del Tribunal Trigésimo de Sustanciación y Ejecución del Circuito Judicial del Trabajo del Área Metropolitana de Caracas de fecha 27 de abril de 2009, explicada en páginas anteriores.

3.2 Proveedores de Certificados (PROCERT) C.A

Proveedor privado de servicios de certificación electrónica, acreditado por SUSCERTE según Providencia Administrativa Nº 028 del 14 de julio de 2008, publicada igualmente en la Gaceta Oficial Nº 38.894 del 31 de julio de 2008. Se encuentra ubicada actualmente en el Multicentro Empresarial del Este, Torre Libertador, núcleo "B", piso 13, oficina B-12, Chacao, Caracas.

Este PSC, tiene como misión:

> Garantizar al cliente un servicio con los más altos estándares de calidad, seguridad, oportunidad, rentabilidad, ética y eficacia como proveedor de certificaciones electrónicas y consultoría, orientados al logro y consecución de sus objetivos, asegurando el cumplimiento del marco legal y tecnológico aplicable a la materia (PROCERT C.A, Página Web en línea).

De igual manera, sus valores como empresa son:

> Ética: En la gestión regular de la empresa y en las relaciones con proveedores y usuarios.
> Economía: En la búsqueda de soluciones eficientes y con un costo razonable en función de la operación.
> Innovación: En la búsqueda de facilidades o soluciones integrales o modulares que simplifiquen el proceso general de la empresa para con sus proveedores y usuarios.
> Seguridad: En el mantenimiento de la información almacenada y en los mecanismos y procedimientos de protección de la información (Ob. Cit).

3.2.1 Del procedimiento para obtener certificados por parte de PROCERT C.A.

Este proveedor de certificados en Venezuela, ofrece sus servicios vía web (www.procert.net.ve) y a través de esta plataforma y de acceder a la misma, el usuario escoge el tipo de certificado (persona natural, profesional, titulado, representante legal de empresa pública o privada), eligiendo a su vez el tipo de contratación electrónica. En esa misma plataforma el usuario podrá conocer las condiciones y el costo de los pagos (que puede realizar directamente a través de la plataforma del banco mercantil). Posteriormente el usuario es contactado por parte de PROCERT para la consignación y verificación de la documentación y emitir el certificado electrónico a través de un Pen-drive, e-token.

Urdaneta (2010:29) expresa: "…a la fecha Procert, ha vendido y emitido certificados

electrónicos a la PYME, al Banco del Pueblo, a personas naturales y a representantes de empresas públicas y privadas".

En atención a ambos proveedores, se puntualiza que los certificados electrónicos emitidos actualmente por éstos, tienen una duración de un (1) año, "renovable, y su costo con IVA oscila entre Bs.F 325 y BsF.697, dependiendo del número de certificados contratados…" (Urdaneta, 2010:.57).

Con la acreditación de estos proveedores, los venezolanos pueden ahora disfrutar de los beneficios de la seguridad que amerita la realización de operaciones en internet y en consecuencia, cualquier certificado electrónico emitido por alguno de aquellos pasa a constituir plena prueba de acuerdo a lo estipulado por el Decreto-LMDFE para los mensajes de datos y las firmas electrónicas que hayan sido certificadas por un proveedor de servicios con plena condición operacional. Ambos proveedores se encuentran inmersos en la Cadena de Confianza Nacional y por lo tanto, son los únicos legitimados para ofrecer servicios de certificación electrónica a todos los usuarios, de acuerdo a lo establecido por el ordenamiento jurídico venezolano. De igual manera es importante acotar que el 17 de julio del año 2009, se dio lugar a la renovación de la acreditación de ambos proveedores de servicios de certificación electrónica, de allí que se muestre de forma evidente el cumplimiento efectivo del Reglamento Parcial del Decreto-LMDFE tanto por parte de SUSCERTE como por la FII y PROCERT C.A.

4. Garantías y desventajas que provee a los usuarios el sistema de certificación electrónica

El sistema de certificación electrónica se ha creado con la firme convicción de impulsar el uso adecuado de las TIC y para contribuir con el desarrollo armonioso de las mismas. Por consiguiente, es de hacer las garantías que provee dicho sistema, entre las que se tiene:

- Ofrece seguridad suficiente para evitar que el mensaje de datos y la firma electrónica sean alterados durante su transmisión, avalando así la confidencialidad, probidad y autenticidad de la información con lo que se conforma la garantía de integridad.

- Declara eficientemente la identidad del signatario del mensaje de datos, lo cual constituye la garantía de autoría.

Gracias a estas garantías se fomenta la rápida y segura incorporación de los avances tecnológicos a las actividades empresariales, así como las que crean vinculación entre los usuarios y el sistema judicial en lo que respecta a la promoción de pruebas en litigios.

Sin embargo, y a pesar de estas garantías, también se presentan circunstancias que limitan el uso de este sistema, tales como:

- El costo que implica para el usuario la utilización de los certificados electrónicos,

pues en todo caso deberá ser sufragado por quien lo utiliza y espera que con ello, a futuro, se evite la existencia de un conflicto, o más aún, en caso de que exista, poder resolverlo con una herramienta eficaz

- La certificación electrónica no garantiza la legalidad del documento electrónico, por cuanto la actuación de los proveedores de servicios de certificación es meramente técnica, no jurídica. Esto es así pues la información contenida en el contrato electrónico les es desconocida y por consiguiente, les es ajena; además, el contrato electrónico no se otorga con la intervención de un proveedor de servicios de certificación electrónica.

En Venezuela hay retraso tecnológico del poder judicial, así como también desconocimiento de parte de muchos magistrados, abogados y litigantes, acerca de las nuevas tecnologías. Se evidencia cotidianamente que el sistema de administración de justicia venezolano es eminentemente escrito y a pesar del importante avance que implica la promulgación del Decreto-LMDFE, lamentablemente, de la configuración actual de los procedimientos judiciales se infiere lo difícil que puede resultar acreditar ante un Juez o árbitro la existencia de una transacción de naturaleza electrónica, su incumplimiento o extinción, así como cualquier otro hecho jurídicamente relevante que haya ocurrido a través de Internet. Por supuesto, la aptitud probatoria de los mensajes de datos quedó solventada con el Decreto-LDMFE, pero aún así no se estableció en el mismo la forma en cómo debe desenvolverse éste como medio probatorio en un proceso diseñado por un legislador que no tomó en cuenta esta novedad.

No obstante, resultan mayores los beneficios que las desventajas que brinda la certificación electrónica, ya que a pesar de su costo puede incluso resultar mucho más costoso la transmisión de información en redes abiertas sin cumplir con los estándares de seguridad necesarios. Si se llegaren a producir controversias a raíz de ese procedimiento, sería difícil probar judicialmente la veracidad de la información contenida en el mensaje de datos que podría estar compuesto por un correo electrónico, por ejemplo, así como también se haría cuesta arriba identificar al signatario del mensaje frente a un Tribunal. La idea se cierne en garantizar un uso adecuado de la tecnología a través de la aplicación correcta de las leyes especiales que regulan la materia.

5. Reflexión final

El sistema de certificación electrónica aplicado en Venezuela es considerado el procedimiento que mayores garantías brinda en el ámbito de las redes abiertas, gracias a la presencia de los proveedores de servicios de certificación electrónica acreditados por SUSCERTE. Los únicos proveedores acreditados operacionalmente y legitimados para llevar a cabo tal procedimiento dentro de la Cadena de Confianza Nacional, son la Fundación Instituto de Ingeniería (FII) de carácter público y PROCERT C.A de carácter privado y por consiguiente, son los únicos autorizados para emitir certificados electrónicos.

Es necesario reiterar que ha sido enfático y claro el esfuerzo del Estado para garantizar el uso adecuado de las nuevas tecnologías, lo cual se demuestra con la creación de instituciones que coadyuvan a brindar la plataforma técnica

requerida a tal fin y la implementación de providencias administrativas que obligan al uso de la certificación electrónica, lo que evidentemente evitará controversias futuras entre los usuarios que sí cumplen con la normativa establecida y las herramientas ofrecidas. Más allá de las desventajas que trae consigo el uso de los servicios de certificación electrónica, los beneficios que brinda son definitivos y resultan de gran utilidad para los usuarios - y aún más en el campo de las transacciones y negociaciones - quienes a partir de la intervención de los proveedores, colocan sus operaciones en un ambiente seguro que les garantiza la confidencialidad e integridad de la información transmitida en redes abiertas. Por consiguiente, antes de contemplar el gasto económico elevado que implica la utilización de estos servicios, es aún más importante que los usuarios visualicen todos los inconvenientes futuros que podrán ahorrarse.

Finalmente, es menester referirse a que sería un complemento ideal para la legislación venezolana la instauración de un sistema único probatorio para los mensajes de datos y firmas electrónicas, de esta manera no se conduciría un proceso simplemente basado en pruebas libres, elementos de convicción y sana crítica del Juez. Sin embargo, muchos funcionarios no poseen los conocimientos adecuados sobre la materia, por lo que urge la preparación académica para la capacitación de profesionales en esta área, no sólo para los abogados en libre ejercicio, sino sobre todo, para los funcionarios públicos a fin de que puedan aplicar la justicia adecuadamente.

De la misma forma, es sumamente necesaria una mayor difusión de la información relativa a la materia, para que el ciudadano común tenga pleno conocimiento de sus derechos y deberes en el mundo del ciberespacio; no sólo información de carácter jurídico, sino también del tipo técnico para mejorar y procurar un uso óptimo de la tecnología de punta en la satisfacción de las necesidades de la sociedad. Dicha difusión se puede llevar a cabo a través de talleres universitarios dirigidos no sólo a los profesionales inmersos en el mundo de la tecnología, sino al público general para que conozca las bondades, las herramientas legales y tecnológica con que cuenta, los sistemas de seguridad, y porque no, los defectos y desventajas de la Internet para crear mayor conciencia ciudadana de su utilización.

Bibliografía

- Centeno, A. (2009). *Análisis del reconocimiento jurídico otorgado por la ley venezolana a los mensajes de datos y firmas electrónicas*. Trabajo Especial de Grado, no publicado. Universidad de los Andes, Mérida.
- Chacón, N. (2005). *La aplicación de los sistemas de certificación electrónica en la actividad comercial*. Universidad Central de Venezuela. Departamento de Publicaciones Facultad de Ciencias Jurídicas y Políticas. Caracas.
- Comisión Nacional de Casinos, Salas de Bingo y Máquinas Traganíqueles Nº 052. (2010). *Gaceta Oficial de la República Bolivariana de Venezuela, 39.449,* Junio 18, 2010.
- Decreto con Fuerza de Ley de Registro y del Notariado. (2006). *Gaceta Oficial de la República Bolivariana de Venezuela, 5.833*, Diciembre 22.

• Decreto-Ley Sobre Mensajes de Datos y Firmas Electrónicas. (2001). *Gaceta Oficial de la República Bolivariana de Venezuela, 37.148,* Febrero 28.
• Fundación Instituto de Ingeniería FII. (2009). [Página Web en Línea]. Disponible: http://www.fii.org/fii/php/index.php [Consulta: 19 diciembre 2009]
• Madrid, A. (2001). *Aspectos jurídicos de la identificación en el comercio electrónico*. Ponencia presentada en las Primeras Jornadas celebradas en la Universidad Carlos III, Madrid.
• Pinochet, R. (2001). *Contratos electrónicos y defensa del consumidor*. Madrid: Marcial Pons, Ediciones Jurídicas y Sociales S.A.
• Providencia Administrativa Nº 027. Gaceta Oficial de la República Bolivariana de Venezuela, Nº 38.894, Julio 31, 2010.
• Proveedores de Certificados PROCERT C.A. (2009). [Página Web en Línea]. Disponible: http://www.procert.net.ve/index.asp.
• Superintendencia de Certificación Electrónica (SUSCERTE) (2010). *Gaceta Oficial de la República Bolivariana de Venezuela 39.432,* Nº 004-10. Mayo 26.
• Recalde, A. (2006). *Comercio y Contratación Electrónica.* Compendio de informática y derecho. España: Cátedra de Derecho Mercantil. Universidad Jaume I Castellón.
• Reglamento Parcial del Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas (Decreto Nº 3.335) (2004, Diciembre 12). *Gaceta Oficial de la Republica Bolivariana de Venezuela, 38.086,* Diciembre 14, 2004.
• Rodríguez, D. (2001). *Los prestadores de servicios de certificación electrónica*.: Editorial Aranzadi S.A. Navarra, España.
• Superintendencia de Servicios de Certificación Electrónica. (2010[a]). [Página Web en Línea]. Disponible: http://www.suscerte.gob.ve/.
• Superintendencia de Certificación Electrónica (2010[b]). *Infraestructura Nacional de Certificación Electrónica: Estructura, certificados y listas de certificados revocados.* En *SUSCERTE* [Página Web en línea]. Disponible: http://www.suscerte.gob.ve/.
• Superintendencia de Certificación Electrónica (2010[c]). *Guía de Evaluación de Credenciales de los Proveedores de Servicios de Certificación Electrónica para la Acreditación*. En *SUSCERTE* [Página Web en línea]. Disponible: http://www.suscerte.gob.ve/
• Tribunal Supremo de Justicia. (2010). [Página Web en Línea]. Disponible: http://www.tsj.gov.ve/decisiones/2009-2010.
• Urdaneta, J. (2010).Los Mensajes de Datos y la Firma Electrónica, (Seguridad Jurídica que ofrecen y valor probatorio). Academia de Ciencias Políticas y Sociales. Caracas.